(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 45 924 A 1**

(51) Int. Cl.[7]:
G 06 F 17/60
H 04 L 9/32

(21) Aktenzeichen: 100 45 924.2
(22) Anmeldetag: 14. 9. 2000
(43) Offenlegungstag: 4. 4. 2002

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Grünzig, Stefan, 85402 Kranzberg, DE; Scheybani, Tschangiz, Dr., 81675 München, DE

(56) Entgegenhaltungen:
DE 197 18 103 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Absichern einer Transaktion auf einem Computernetzwerk

(57) Es wird ein Verfahren zum Absichern einer Transaktion über ein Computernetzwerk beschrieben, bei dem an einen Servicenutzer ein einmaliges Transaktionskennwort übermittelt wird, welches zur Transaktionsbestätigung vom Servicenutzer über das Computernetzwerk an einen Serviceanbieter übermittelt wird. Das Transaktionskennwort wird dabei über ein Mobilfunknetz an ein mobiles Kommunikationsendgerät des Servicenutzers übermittelt, wobei vor einer Übermittlung des Transaktions-Kennworts an den Servicenutzer eine Überprüfung persönlicher Servicenutzer-Daten erfolgt.

DE 100 45 924 A 1

Beschreibung

[0001] Die Erfindung betrifft ein Verfahren zum Absichern einer Transaktion auf einem Computer- oder ähnlichem Netzwerk, beispielsweise im Internet oder auch in einem größeren organisationsinternen Intranet, bei dem an einen Servicenutzer ein einmaliges Transaktionskennwort übermittelt wird, welches zur Transaktions-Bestätigung vom Servicenutzer über das Computernetzwerk an einen Serviceanbieter übermittelt wird.

[0002] Ein derartiges Verfahren wird zur Zeit beispielsweise bei dem üblichen Online-Banking-Verfahren genutzt. Der Bankkunde bekommt hierbei außer der PIN zusätzliche Transaktionsnummern, sogenannte TAN, zugesandt, die jeweils nur für eine einzige Transaktion verwendet werden können und anschließend ihre Gültigkeit verlieren. Nur bei Übereinstimmung der PIN und der TAN mit den beim Online-Banking-Anbieter hinterlegten Werten wird die Transaktion durchgeführt. Da die TAN nur ein einziges Mal verwendet wird, ist sichergestellt, dass Unbefugte, denen es gelingt, den Datentransfer zwischen Bank und Kunden auszuspionieren, mit den ermittelten Daten keinen Missbrauch treiben können. Die TAN bietet somit eine zusätzliche Sicherheit für den Kunden, da so ein Missbrauch der Online-Bankverbindung erheblich reduziert wird. Zum anderen bietet sie aber auch eine zusätzliche Sicherheit für den Online-Banking-Anbieter, da durch die Zusammenwirkung von richtiger PIN und richtiger TAN die Authentizität des Kunden bestätigt wird. Derartige vom Online-Banking bekannte Verfahren sind selbstverständlich auch anwendbar, um Transaktionen im Zusammenhang mit anderen Geschäften im Internet, beispielsweise beim Kauf von Waren, auszuführen.

[0003] Um zu verhindern, dass Unbefugte in den Besitz der TAN gelangen, solange sie noch für eine Transaktion verwendet werden kann, erfolgt die Zusendung der TAN an den Kunden bisher per Brief unter entsprechenden Sicherheitsbedingungen. Wegen des erheblichen Aufwands und der Dauer eines postalischen Versands werden hierbei üblicherweise an den Kunden gleich mehrere gültige TAN, beispielsweise 40 verschiedene TAN, versandt, die der jeweiligen PIN des Kunden zugeordnet sind. Der Kunde muss die 40 TAN an gesicherter Stelle aufbewahren und kann jede dieser TAN einmal verwenden. Sobald der Kunde alle TAN verbraucht hat, kann er neue TAN von seiner Bank anfordern.

[0004] Es ist offensichtlich, dass die Verwaltung solcher TAN, besonders für den Kunden, äußerst unkomfortabel ist. In der Regel besteht die Möglichkeit, die erhaltenen TAN im Computer des Kunden mit geeigneter Software abzuspeichern. Es wird dann automatisch bei Durchführung einer Transaktion vom Online-Banking-Programm eine der gespeicherten TAN verwendet und anschließend als gelöscht gekennzeichnet. D. h. es werden automatisch zum richtigen Zeitpunkt innerhalb einer Transaktion PIN und TAN übertragen, ohne dass der Kunde direkt eingreifen muss. Die Abspeicherung der TAN und/oder der PIN birgt jedoch die erhebliche Gefahr, dass diese sensiblen Daten durch Unbefugte auf dem Computer des Kunden, beispielsweise durch sogenannte "Trojanische Pferde" oder ähnliche Programme, ausspioniert werden und dann für einen Missbrauch verwendet werden können. Die sichererè Alternative hierzu bedeutet jedoch, dass der Kunde die TAN nicht in seinem Rechner speichert, sondern statt dessen in schriftlicher Form an sicherer Stelle aufbewahrt. Da es für den Kunden in der Regel aber unpraktikabel ist, sich mehrere dieser TAN zu merken, bedeutet dies gleichzeitig, dass der Kunde die schriftlich notierten TAN mit sich führen muss, wenn er von verschiedenen Orten und unterschiedlichen Rechnern aus seine Bankgeschäfte durchführen will. Zudem besteht bei dieser Aufbewahrung auch die Möglichkeit, dass die TAN dem Kunden beispielsweise durch Diebstahl abhanden kommt oder verloren geht und in unbefugte Hände gelangt.

[0005] In der US 5,809,144 wird ein Verfahren zum Verkauf und zur Lieferung von. Waren im Internet genannt, bei dem zur Absicherung von Kunden und Verkäufern gegeneinander sowie zur Sicherung gegen Abhören und Missbrauch von Daten ein Verfahren vorgeschlagen wird, das die Übersendung mehrerer kryptographischer Checksummen sowie einer Signatur einschließt. Dieses Verfahren ist jedoch äußerst aufwendig und rechenintensiv.

[0006] Es ist Aufgabe der vorliegenden Erfindung, eine Alternative zum genannten Stand der Technik zu schaffen, mit der auf einfache und sichere Weise eine Absicherung einer Transaktion, beispielsweise einer Zahlungstransaktion, über ein Computernetzwerk bzw. ein Netzwerk, welches zum Austausch von Daten geeignet ist (z. B. Internet-Nutzung über Mobilfunk), möglich ist.

[0007] Diese Aufgabe wird durch ein Verfahren gemäß Patentanspruch 1 gelöst. Die abhängigen Ansprüche enthalten vorteilhafte Weiterbildungen und Ausgestaltungen des erfindungsgemäßen Verfahrens.

[0008] Bei dem erfindungsgemäßen Verfahren wird ebenfalls an den Servicenutzer, d. h. den Kunden, ein einmaliges Transaktionskennwort übermittelt, das dieser zur Transaktionsbestätigung über das Computernetzwerk an einen Serviceanbieter zurückübermittelt, um eine Zahlung durchzuführen. Bei dem Transaktionskennwort kann es sich um ein beliebiges Kennwort handeln. Vorzugsweise handelt es sich um eine Nummer, d. h. eine übliche TAN. Zur Erhöhung der Sicherheit werden dabei vor der Übermittlung eines Transaktions-Kennworts an einen Servicenutzer dessen persönliche Daten überprüft. Hierbei handelt es sich in erster Linie um diejenigen Daten, die für die Transaktion benötigt werden, beispielsweise um den Namen, die Adresse, eine Kreditkartennummer und eine Mobilfunkteilnehmernummer des Kommunikationsendgeräts des Servicenutzers. Neben diesen Daten können selbstverständlich, alternativ oder zusätzlich zum Namen und zur Adresse, weitere Daten, beispielsweise eine Ausweis- oder Passnummer des Servicenutzers, registriert werden.

[0009] Das Transaktionskennwort dient wie in den eingangs genannten Fällen der Absicherung des Servicenutzers und zur Authentisierung des Servicenutzers gegenüber dem Serviceanbieter. Es wird nur einmal für eine einzige Transaktion verwendet und verliert anschließend seine Gültigkeit. Das Transaktionskennwort wird vom Serviceanbieter mit einem dort gespeicherten Transaktionskennwort verglichen und nur bei Übereinstimmung, d. h. bei Rücksendung des richtigen Transaktions-Kennworts, wird die Transaktion durchgeführt. Die Übersendung des Transaktions-Kennworts zum Servicenutzer erfolgt nicht über das Computernetzwerk, sondern über ein Mobilfunknetz an ein mobiles Kommunikationsendgerät des Kunden. Bei dem Mobilfunknetz kann es sich um ein beliebiges Mobilfunknetz, beispielsweise GSM oder UMTS, handeln. Der Begriff Mobilfunknetz umfasst hierbei auch entsprechende Pager-Netze. Bei dem mobilen Kommunikationsendgerät handelt es sich beispielsweise um ein handelsübliches Mobilfunkgerät, einen Pager oder einen PDA mit entsprechender Mobilfunk-Funktion.

[0010] Der Servicenutzer kann das Transaktionskennwort direkt vom Serviceanbieter erhalten. Selbstverständlich ist es auch möglich, dass das Transaktionskennwort von einer anderen Stelle, beispielsweise einer Kreditkarten-Organisation oder einem Mobilfunknetz-Anbieter, welcher mit dem

Serviceanbieter in Verbindung steht, an den Servicenutzer übermittelt wird. Entscheidend ist, dass hier, anders als bei der eingangs genannten US 5,809,144 die sicherheitssensiblen Daten, die der Servicenutzer zur Bestätigung einer Transaktion an den Serviceanbieter über das Computernetzwerk versenden soll, nicht über das gleiche Netzwerk erfolgt, sondern dass zur Übersendung des Transaktions-Kennworts an den Servicenutzer ein völlig anderer Weg verwendet wird. Dies erhöht die Sicherheit erheblich, da für einen Missbrauch durch eine unbefugte Person nun nicht mehr nur Name, Adresse usw. des Servicenutzers bekannt sein müssen, sondern er sich auch noch im Besitz des Kommunikationsendgeräts des Servicenutzers befinden muss.

[0011] Da bei dem erfindungsgemäßen Verfahren die Übersendung des Transaktions-Kennworts, anders als bei einer Übersendung mit spezieller Post wie beim bisherigen Online-Banking-Verfahren, schnell und unkompliziert ist, ist es möglich, dass das Transaktionskennwort jeweils direkt während oder unmittelbar vor einer Transaktion an den Service-Nutzer übermittelt wird. D. h. es ist nicht mehr nötig, dass vorab mehrere Nummern übermittelt werden. Somit ist es auch nicht mehr erforderlich, dass der Service-Nutzer mehrere Nummern sicher so verwahrt, dass er die Nummer zum geeigneten Zeitpunkt zur Hand hat. Damit ist gleichzeitig ausgeschlossen, dass Unbefugte in den Besitz eines Blocks von TAN kommen.

[0012] Zur Überprüfung dieser Daten wird dann ein Konsistenz-Abgleich zwischen dem Serviceanbieter, einem Mobilfunknetz-Anbieter und einer Kreditkartengesellschaft durchgeführt, d. h. der Serviceanbieter führt beispielsweise einen Abgleich der Daten mittels einer Datenbankabfrage beim Mobilfunknetz-Anbieter und einer gleichzeitigen Datenbank-Abfrage bei der Kreditkartengesellschaft durch. Er stellt so sicher, dass die Mobilfunk-Teilnehmernummer und die Kreditkartennummer zum selben Servicenutzer gehören. Gleichzeitig kann selbstverständlich auch eine Abfrage über die Zahlungsfähigkeit des Servicenutzers über die Kreditkarte erfolgen.

[0013] Nur nach einem erfolgreichen Konsistenz-Check der Servicenutzer-Daten wird der Service schließlich freigeschaltet, und dem Servicenutzer wird ein Transaktionskennwort übermittelt, mit dem er schließlich die Transaktion durchführen kann.

[0014] Da die Übermittlung sämtlicher Servicenutzer-Daten sowie ein entsprechender Konsistenz-Abgleich durch den Serviceanbieter während jeder einzelnen Transaktion relativ aufwendig ist, erfolgt vorzugsweise vor einer erstmaligen Transaktion ein Registriervorgang, bei dem zumindest ein Teil der Servicenutzer-Daten an den Serviceanbieter übermittelt werden. Es erfolgt dann sofort die Überprüfung der Servicenutzer-Daten, beispielsweise der vollständige Konsistenz-Abgleich. Bei erfolgreicher Registrierung wird dem Service-Nutzer schließlich eine persönliche Identifizierungsnummer, im Folgenden PIN genannt, übermittelt, die diesem Servicenutzer zugeordnet ist. Bei einer späteren Transaktion wird dann zunächst die PIN vom Servicenutzer an den Serviceanbieter übermittelt, womit dieser automatisch über die Daten des aktuellen Service-Nutzers informiert ist. Vom Service-Anbieter wird dann vorzugsweise anstelle der kompletten Servicenutzer-Daten nur noch die PIN überprüft. Selbstverständlich ist es aber auch möglich, dass bei jeder Sitzung der Servicenutzer erneut seine Daten gemeinsam mit der PIN eingibt und sowohl die Servicenutzer-Daten als auch die PIN überprüft werden.

[0015] Die persönliche Identifizierungsnummer kann beispielsweise – wie auch das Transaktionskennwort – über ein Mobilfunknetz an das mobile Kommunikationsendgerät des Kunden übermittelt werden.

[0016] Bei einem weiteren bevorzugten Ausführungsbeispiel werden vom Servicenutzer unter Angabe der PIN dem Serviceanbieter Servicenutzer-Daten übermittelt, die bei nachfolgenden Transaktionen verwendet werden. Hierbei handelt es sich sozusagen um eine zweite Registrierungsstufe, bei der dem Serviceanbieter die Servicenutzer-Daten übermittelt werden, die er bei der ersten Registrierung nicht erhalten hat. Alternativ ist auf diese Weise natürlich auch eine Änderung von Servicenutzer-Daten möglich, beispielsweise wenn der Servicenutzer ein anderes Kommunikationsendgerät mit einer Mobilfunk-Teilnehmernummer verwenden möchte oder eine andere Kreditkarte mit einer anderen Kreditkartennummer zur Zahlung verwenden möchte.

[0017] Selbstverständlich ist bei jeder Registrierung eine Eingabe verschiedener Kreditkartennummern, beispielsweise von verschiedenen Kreditkartengesellschaften, oder auch eine Eingabe von mehreren verschiedenen Mobilfunkteilnehmern, beispielsweise von verschiedenen Kommunikationsendgeräten, möglich. Der Servicenutzer kann dann bei einer späteren Nutzung des Service jederzeit unter den verschiedenen Möglichkeiten wählen.

[0018] Die Übermittlung der Servicenutzer-Daten und/oder der PIN über das Computernetzwerk erfolgt vorzugsweise auf gesicherte Weise, d. h. es wird ein gesicherter Kanal, beispielsweise das SSL-Verfahren, verwendet, bei dem diese sensiblen Daten verschlüsselt übermittelt werden.

[0019] Das Transaktionskennwort bzw. die persönliche Identifizierungsnummer wird auf das mobile Kommunikationsendgerät des Servicenutzers vorzugsweise als Textnachricht, beispielsweise SMS, übermittelt. Dieses Verfahren ist äußerst kostengünstig, da es nur wenig Übertragungskapazität benötigt. Der Servicenutzer kann die PIN bzw. das Transaktionskennwort im Klartext vom Display seines Kommunikationsendgeräts ablesen und an entsprechender Stelle in einer Eingabemaske an seinem PC eingeben.

[0020] Bei einem bevorzugten Ausführungsbeispiel erhält der Servicenutzer die PIN von einem Mobilfunknetz-Anbieter oder einem damit verbundenen Dienstleister. Dem Mobilfunknetz-Anbieter bzw. dem damit verbundenen Dienstleister sind Name, Adresse und Mobilfunk-Teilnehmernummer des Servicenutzers bereits bekannt. Unter Angabe dieser PIN übermittelt dann der Servicenutzer dem Serviceanbieter eine Kreditkartennummer, die bei nachfolgenden Transaktionen verwendet wird. Der Serviceanbieter überprüft die PIN durch Vergleich mit der PIN, die er gemeinsam mit den persönlichen Daten ebenfalls vom Mobilfunknetz-Anbieter oder dem damit verbundenen Dienstleister erhalten hat und ordnet diesen Daten die Kreditkartennummer zu und/oder führt einen entsprechenden Konsistenz-Abgleich durch eine Datenbank-Abfrage bei der betreffenden Kreditkarten-Organisation durch. Alternativ ist es selbstverständlich auch möglich, dass der Servicebetreiber die erhaltene PIN lediglich an den Mobilfunknetz-Anbieter oder den damit verbundenen Dienstleister zur Überprüfung weiterleitet und von diesem lediglich eine Information zurückerhält, dass die Daten in Ordnung sind. Bei erfolgreicher Überprüfung wird der Service freigeschaltet und kann jederzeit vom Servicenutzer genutzt werden. Der Service funktioniert in diesem Fall nur mit der Mobilfunk-Teilnehmernummer, über die der Nutzer ursprünglich beim Mobilfunknetz-Anbieter bekannt ist. Die Kreditkartennummer kann mit diesem Verfahren jederzeit vom Servicenutzer geändert werden.

[0021] Bei einem alternativen Verfahren wird die PIN von einer Kreditkartenorganisation oder einem damit verbundenen Dienstleister an den Servicenutzer übermittelt. In diesem Fall kann der Servicenutzer mit der erhaltenen PIN die Registrierung beim Serviceanbieter durchführen und dabei

seine Mobilfunk-Teilnehmernummer angeben. Auch hier erfolgt wie im vorherigen Fall zunächst eine Überprüfung aller Daten. Anschließend wird der Service freigeschaltet, wobei in diesem Fall der Service nur in Verbindung mit der anfangs bekannten Kreditkartennummer funktioniert, unter der der Servicenutzer auch bei der Kreditkartenorganisation gemeldet ist, die die PIN übermittelt hat. Die Mobilfunk-Teilnehmernummer kann jederzeit vom Servicenutzer durch eine erneute Registrierung mit der PIN geändert werden.

[0022] Das erfindungsgemäße Verfahren zur Sicherung von Transaktionen kann bei beliebigen Vorgängen eingesetzt werden. Es kann beispielsweise direkt im Online-Banking-Verfahren verwendet werden. Außerdem kann es auch für Einkäufe über das Internet und die darauf folgende Zahlung verwendet werden. Der Serviceanbieter braucht hierbei nicht zwangsläufig mit dem Internetshop-Betreiber identisch zu sein. Es muss lediglich eine entsprechende – direkte oder indirekte – Verbindung zwischen Serviceanbieter und Shop-Betreiber bestehen, d. h. Shop-Betreiber und Serviceanbieter sind beispielsweise Vertragspartner oder sind über einen gemeinsamen Vertragspartner miteinander verbunden. Bei dem Serviceanbieter kann es sich beispielsweise auch um die Kreditkartenorganisation oder den Mobilfunknetz-Anbieter selbst handeln. Es kann sich aber auch um eine vollständig eigenständige Organisation handeln, die mit den verschiedenen anderen Organisationen und Betreibern in Geschäftsverbindung steht.

[0023] Das erfindungsgemäße Verfahren bietet außerdem die Möglichkeit, dass mit dem Transaktionskennwort und/oder der PIN weitere Informationen an das mobile Kommunikationsendgerät des Servicenutzers übermittelt werden. Bei diesen zusätzlichen Informationen kann es sich beispielsweise um aktuelle Informationen über den Dienst selbst handeln. Es kann sich aber auch um Werbung oder ähnliches handeln. In diesem Fall ist beispielsweise auch eine Finanzierung des Service über die mit dem Transaktionskennwort oder der PIN gesendete Werbung möglich, so dass für die Shop-Betreiber, den Servicenutzer, für die beteiligte Kreditkartenorganisation oder den Mobilfunknetz-Anbieter keine zusätzlichen Kosten entstehen.

[0024] Da die Nachrichten auf ein mobiles Kommunikationsendgerät über ein Mobilfunknetz übermittelt werden, ist das Verfahren äußerst flexibel, d. h. der Servicenutzer ist nicht darauf angewiesen, die Transaktionen von seinem eigenen PC an einem festen Standort durchzuführen, sondern kann jeden beliebigen ihm zur Verfügung stehenden Rechner nutzen. Das erfindungsgemäße Verfahren ist folglich überall dort einsetzbar, wo der Kunde mit seinem mobilen Kommunikationsendgerät erreichbar ist, d. h. bei Verwendung eines Mobilfunkgeräts auch international dort, wo Roaming möglich ist. Es wird keine spezielle Infrastruktur wie beispielsweise ein Smart-Card-Terminal am gerade vom Kunden benutzten Computer benötigt.

[0025] Das gesamte Verfahren der Registrierung der Kunden, der Übermittlung von Identifizierungsnummern sowie von Transaktions-Kennworten sowie die Überprüfung der verschiedenen Daten kann vollautomatisch über einen geeigneten Computer, beispielsweise einen Server des Servicebetreibers, erfolgen, auf dem ein entsprechendes Computerprogramm implementiert ist.

[0026] Die Erfindung wird im Folgenden noch einmal anhand konkreter Ausführungsbeispiele erläutert:

Bei den folgenden Ausführungsbeispielen wird jeweils davon ausgegangen, dass es sich bei dem Transaktionskennwort um eine Nummer, d. h. eine TAN, handelt. Außerdem wird davon ausgegangen, dass die Übermittlung der verschiedenen TAN und der PIN über SMS auf ein Mobilfunk gerät des Servicenutzers erfolgt. Ebenso erfolgt die letztendliche Zahlung immer über eine Kreditkarte des Servicenutzers, wobei die Belastung der Kreditkarte des Servicenutzers durch den Serviceanbieter auf eine allgemein bekannte, übliche Weise erfolgen kann. Selbstverständlich ist die Erfindung nicht auf diese konkreten Ausführungsbeispiele beschränkt.

[0027] Beim ersten Ausführungsbeispiel handelt es sich um einen Spontankauf eines bisher beim Serviceanbieter nicht registrierten Servicenutzers.

[0028] Voraussetzung für die Abwicklung einer sicheren Kreditkartenzahlung ist auch hier ein Konsistenz-Abgleich der Servicenutzer-Daten, nämlich der Kreditkartennummer, der Mobilfunknummer sowie der Adresse und des Namens des Servicenutzers. Dieser Konsistenz-Abgleich erfolgt zwischen Serviceanbieter, Mobilfunknetz-Anbieter und Kreditkartenorganisation.

[0029] Während des Shoppens am PC, nach Aktivieren eines Bezahlvorgangs, wird der Servicenutzer auf den Internet-Server bzw. eine Website des Servicebetreibers weitergeleitet. Hier gibt der Servicenutzer in einer entsprechenden Dialogmaske auf seinem PC seine Kreditkartennummer und seine Mobilfunknummer ein, die mittels eine sicheren Übertragung, beispielsweise mittels SSL, zum Server übertragen werden. Name und Adresse können hier ebenfalls eingegeben werden und mit übertragen werden. In der Regel sind die Daten aber bereits auf der Website des Internet-Shops angegeben worden, da diese Daten ja auch zur Auslieferung der Ware benötigt werden. Diese Daten können daher beim Weiterleiten des Servicenutzers auf den Internet-Server bzw. die Website des Servicebetreibers auch direkt vom Shop-Betreiber an den Servicebetreiber weitergegeben werden.

[0030] Der Serviceanbieter führt dann den notwendigen Abgleich aller Servicenutzer-Daten mittels einer entsprechenden Datenbank-Abfrage beim Mobilfunkbetreiber und einer gleichzeitigen Datenbankabfrage bei der Kreditkartengesellschaft durch. Bei positivem Abfrageergebnis ist der Service freigeschaltet, und der Servicenutzer erhält eine einmalige TAN für diesen Bezahlvorgang mittels SMS auf sein Mobilfunkgerät zugeschickt. Es erfolgt dann die Eingabe der TAN durch den Servicenutzer am PC in eine entsprechende Eingabemaske. Schließlich wird die TAN vom PC zum Hintergrundsystem, beispielsweise zum Internet-Server des Servicebetreibers, gesendet. Es erfolgt dann ein Vergleich der an den Servicenutzer gesendeten TAN mit der dort hinterlegten TAN. Bei erfolgreichem Vergleich erfolgt die Belastung auf dem Kreditkartenkonto des Servicenutzers. Der Servicenutzer selbst erhält eine Bestätigung der erfolgreichen Kreditkartenzahlung.

[0031] Beim zweiten Ausführungsbeispiel wird davon ausgegangen, dass der Servicenutzer bereits beim Serviceanbieter zuvor registriert ist und im Zuge des Registrierungsvorgangs eine eindeutige PIN erhalten hat.

[0032] Hierbei meldet sich der registrierte Servicenutzer während des Shoppens am PC auf dem Internetserver des Servicebetreibers mittels seiner PIN über einen sicheren Kanal an. Anschließend wird die PIN beim Servicebetreiber überprüft und der Service für die aktuelle Sitzung freigeschaltet. Der Servicenutzer hat dann beispielsweise die Möglichkeit, innerhalb eines Internet-Shop einen Warenkorb zusammenzustellen. Nachdem der Warenkorb zusammengestellt wurde, muss dann der Servicenutzer nur noch den Bezahlvorgang, beispielsweise mittels eines Button auf der Website des Serviceanbieters, aktivieren. Daraufhin wird sofort die TAN auf das Mobilfunkgerät des Servicenutzers übermittelt. Auch hier wird dann die TAN vom Servicenutzer am PC in eine Eingabemaske eingegeben und über das Computernetzwerk zurückübermittelt. Nach erfolgreichem Vergleich der TAN wird wiederum das Kreditkarten-

über ein Mobilfunknetz an ein mobiles Kommunikationsendgerät des Servicenutzers übermittelt wird, **dadurch gekennzeichnet**, dass vor einer Übermittlung des Transaktions-Kennworts an den Servicenutzer eine Überprüfung persönlicher Servicenutzer-Daten erfolgt.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass das Transaktionskennwort während oder unmittelbar vor einer Transaktion an den Servicenutzer übermittelt wird.

3. Verfahren nach einem der Ansprüche 1 bis 2, dadurch gekennzeichnet, dass zumindest ein Teil der Servicenutzer-Daten während einer Transaktion vom Servicenutzer über das Computernetzwerk an den Serviceanbieter übermittelt werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass zumindest ein Teil der Servicenutzer-Daten bei einem ersten Registriervorgang vor einer erstmaligen Transaktion an den Serviceanbieter übermittelt werden und diese Servicenutzer-Daten geprüft werden und dem Servicenutzer bei erfolgter Registrierung eine dem Servicenutzer zugeordnete persönliche Identifizierungsnummer übermittelt wird und bei einer Transaktion die persönliche Identifizierungsnummer vom Servicenutzer an den Serviceanbieter übermittelt wird und vom Serviceanbieter zusammen mit den oder anstelle der Servicenutzer-Daten die persönliche Identifizierungsnummer geprüft wird.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, dass die persönliche Identifizierungsnummer über ein Mobilfunknetz an das mobile Kommunikationsendgerät des Servicenutzer übermittelt wird.

6. Verfahren nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass vom Servicenutzer an den Serviceanbieter unter Angabe der persönlichen Identifizierungsnummer Servicenutzer-Daten übermittelt werden, die bei nachfolgenden Transaktionen verwendet werden.

7. Verfahren nach einem der Ansprüche 2 bis 6, dadurch gekennzeichnet, dass die Servicenutzer-Daten einen Namen und/oder eine Adresse und/oder eine Kreditkartennummer und/oder eine Mobilfunk-Teilnehmernummer des Servicenutzers umfassen.

8. Verfahren nach Anspruch 6 oder 7, dadurch gekennzeichnet, dass der Servicenutzer die persönliche Identifizierungsnummer von einem Mobilfunknetzbetreiber oder einem damit verbundenen Dienstleister übermittelt wird und unter Angabe der persönlichen Identifizierungsnummer vom Servicenutzer dem Serviceanbieter eine Kreditkartennummer übermittelt wird, die bei nachfolgenden Transaktionen verwendet wird.

9. Verfahren nach Anspruch 6 oder 7, dadurch gekennzeichnet, dass der Servicenutzer die persönliche Identifizierungsnummer von einer Kreditkartenorganisation oder einem damit verbundenen Dienstleister übermittelt wird, und unter Angabe der persönlichen Identifizierungsnummer vom Servicenutzer dem Serviceanbieter eine Mobilfunk-Teilnehmernummer übermittelt wird, die bei nachfolgenden Transaktionen verwendet wird.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die Servicenutzer-Daten und/oder die persönliche Identifizierungsnummer gesichert über das Computernetzwerk übermittelt wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass das Transaktionskennwort oder die persönliche Identifizierungsnummer als Textnachricht übermittelt wird.

12. Verfahren nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass mit dem Transaktions-

kennwort und/oder der persönlichen Identifizierungsnummer zusätzliche Informationen zum Kommunikationsendgerät des Servicenutzers übermittelt werden.

Hierzu 1 Seite(n) Zeichnungen

konto das Servicenutzers belastet, und es erfolgt eine Bestätigung der erfolgreichen Kreditkartenzahlung.

[0033] Selbstverständlich ist es möglich, dass der Servicenutzer unter verschiedenen Kreditkartengesellschaften auswählt, von denen er jeweils Kreditkarten besitzt. Dies kann innerhalb einer Eingabemaske auf der Website des Serviceanbieters abgefragt werden. Selbst im Falle einer zuvor erfolgten Registrierung besteht diese Möglichkeit, sofern der Servicenutzer bei der Registrierung die verschiedenen Kreditkartengesellschaften mit den entsprechenden Kreditkartennummern angegeben hat. Ebenso kann zwischen verschiedenen Mobilfunkgeräten mit unterschiedlichen Mobilfunknummern gewählt werden, sofern dies zuvor bei der Registrierung angegeben worden ist.

[0034] Für die Registrierung gibt es ebenfalls mehrere Alternativen, wobei im Folgenden vier verschiedene Beispiele genannt werden.

[0035] Bei der ersten Version kennt der Serviceanbieter den Servicenutzer bereits als Kreditkartenhalter, d. h. es sind ihm Name, Adresse und Kreditkartennummer bekannt. Dies ist beispielsweise dann der Fall, wenn der Servicebetreiber selbst die betreffende Kreditkartenorganisation ist oder mit einer solchen in geschäftlicher Verbindung steht und die Daten untereinander austauscht.

[0036] In diesem Fall bekommt der Servicenutzer von seiner Kreditkartenorganisation oder einem damit verbundenen Dienstleister eine PIN zur Nutzung des Service zugestellt. Mittels dieser PIN kann sich der Servicenutzer auf dem Server des Serviceanbieters einloggen und seine Mobilfunknummer zur Benutzung des Service eingeben. Damit wird der Service freigeschaltet. Der Service funktioniert nur mit der Kreditkartennummer, die dem Serviceanbieter bereits bekannt ist. Die Mobilfunknummer kann jederzeit durch erneutes Einloggen unter Eingabe der PIN geändert werden.

[0037] Bei der zweiten Version kennt der Serviceanbieter den Servicenutzer bereits in seiner Person als Mobilfunknutzer, d. h. dem Serviceanbieter sind Name, Adresse und Mobilfunknummer bekannt. Dies ist beispielsweise der Fall, wenn der Servicebetreiber selbst der Mobilfunknetzbetreiber ist oder mit diesem in Verbindung steht.

[0038] In diesem Fall bekommt der Servicenutzer von seinem Mobilfunknetzbetreiber oder einem damit verbundenen Dienstleister die PIN zur Nutzung des Service zugestellt. Mittels der PIN loggt sich der Servicenutzer wiederum auf dem Server des Serviceanbieters ein und gibt seine Kreditkartennummer zur Nutzung des Service ein. In diesem Fall funktioniert der Service nur mit der dem Serviceanbieter bereits bekannten Mobilfunkteilnehmernummer. Die Kreditkartennummer kann jederzeit unter Eingabe der PIN wieder geändert werden.

[0039] Bei einer dritten Version erfolgt die Registrierung in einem Mobilfunkladen. Hier werden ebenfalls Name, Adresse und Mobilfunknummer registriert, und der Servicenutzer erhält beispielsweise einen PIN-Brief. Diese Registrierung kann auch beim Postboten oder im Postamt erfolgen. Mittels der zugestellten PIN kann sich der Servicenutzer auf dem Server des Serviceanbieters einloggen und wiederum seine Kreditkartennummer zur Nutzung des Service eingeben. Auch dann erfolgt der Service nur mit der anfangs registrierten Mobilfunknummer.

[0040] Selbstverständlich ist bei dieser dritten Alternative auch die Möglichkeit gegeben, dass beispielsweise beim Postboten oder im Postamt anstelle der Mobilfunknummer die Kreditkartennummer mit der betreffenden Kreditkartenorganisation registriert wird und anschließend mittels der PIN die Mobilfunkteilnehmernummer angegeben und gegebenenfalls geändert wird.

[0041] Das vierte Registrierungsbeispiel ist eine reine Online-Registrierung.

[0042] Voraussetzung für diese reine Online-Registrierung ist wiederum ein Konsistenz-Abgleich der angegebenen Servicenutzer-Daten zwischen dem Serviceanbieter, dem betreffenden Mobilfunknetz-Anbieter und der Kreditkartenorganisation.

[0043] Hierbei loggt sich der Servicenutzer auf einer speziellen Registrierungs-Web-Site des Serviceanbieters ein und gibt dort Namen, Adresse sowie Kreditkartennummer und Mobilfunkteilnehmernummer an. Der Serviceanbieter führt anschließend einen Abgleich der Servicenutzer-Daten mittels einer Datenbankabfrage beim Mobilfunknetz-Anbieter und eine Datenbankabfrage bei der Kreditkartengesellschaft durch. Nur bei positiven Abfrageergebnissen ist der Service freigeschaltet, und der Servicenutzer erhält eine PIN zur Nutzung des Service. Diese PIN kann auf beliebigem Wege, beispielsweise per Post, übermittelt werden. Vorzugsweise erfolgt jedoch diese PIN-Übertragung ebenfalls über das Mobilfunknetz auf das Mobilfunkgerät unter der eingegebenen Mobilfunk-Nummer. Die Übertragung der PIN kann hierbei ebenfalls über SMS erfolgen. Dieses Verfahren hat den Vorteil, dass der Servicenutzer nicht erst auf die Zustellung eines Briefs warten muss, sondern die Übermittlung der PIN unmittelbar nach der Online-Registrierung erfolgen kann und somit der Dienst dem Servicenutzer sofort zur Verfügung steht.

[0044] Anhand der Figur wird nachfolgend noch einmal ein weiteres Ausführungsbeispiel für eine Nutzung nach einer zuvor erfolgten Registrierung beschrieben, wobei bei diesem speziellen Ausführungsbeispiel der Internet-Shop (Web-Shop) nicht direkt mit dem Serviceanbieter in Kontakt steht, sondern ein weiterer Dienstleister, hier ein Payment-Service-Provider (PSP) zwischengeschaltet ist.

[0045] Auch hier loggt sich der Servicenutzer zunächst über das Internet beim gewünschten Web-Shop ein und führt dort eine Bestellung aus. Zur Einziehung des dafür fälligen Betrags sendet der Web-Shop den Betrag beispielsweise gemeinsam mit Namen und Adresse des Servicenutzers an den Payment-Service-Provider. Dieser erteilt schließlich dem Serviceanbieter einen Auftrag zur Kundenidentifizierung. Gleichzeitig wird der Servicenutzer automatisch auf die Website des Serviceanbieters weitergeleitet. Hier muß der Nutzer zunächst die PIN zum Freischalten des Bezahlservice angeben. Anschließend werden die Daten bzw. die PIN des Servicenutzers auf Konsistenz überprüft und auch mit den vom Payment-Service-Provider erhaltenen Daten verglichen. Nach erfolgreicher Überprüfung sendet der Serviceanbieter über das GSM-Netz eine TAN an das Mobilfunkgerät des Servicenutzers, der wiederum die TAN vom Display des Mobilfunkgeräts abliest und zur Transaktionsbestätigung an entsprechender Stelle in eine Eingabemaske auf seinem PC eingibt. Die TAN wird dann über das Internet zur Prüfung an den Serviceanbieter gesendet. Bei erfolgreicher Überprüfung der TAN wird dem Payment-Service-Provider ein "Kunde-O.K."-Signal übermittelt. Der Payment-Service-Provider sorgt schließlich für das Einziehen des Betrags von einem Kreditkartenkonto des Servicenutzers und quittiert die erfolgreiche Zahlung an den Web-Shop mit einem "Payment-O.K." Signal.

Patentansprüche

1. Verfahren zum Absichern einer Transaktion über ein Computernetzwerk, bei dem an einen Servicenutzer ein einmaliges Transaktionskennwort übermittelt wird, welches zur Transaktionsbestätigung vom Servicenutzer über das Computernetzwerk an einen Serviceanbieter übermittelt wird, wobei das Transaktionskennwort

- Leerseite -

Nummer: DE 100 45 924 A1
Int. Cl.[7]: G 06 F 17/60
Offenlegungstag: 4. April 2002

FIG.1